|  |  |  |  |
| --- | --- | --- | --- |
| **RIESGOS** | **POSIBILIDADES DE RIESGO** | **IMPACTO** | **MITIGAR ESTOS RIESGOS** |
| **Riesgos de Seguridad** | * Vulnerabilidades en el código * Falta de cifrado * Autenticación débil * Exposición de API * Ataques DDoS | * Fallas como inyección SQL, XSS (Cross-Site Scripting) o manejo inadecuado de datos sensibles. * Datos transmitidos o almacenados sin cifrar pueden ser interceptados. * Uso de contraseñas inseguras o falta de autenticación multifactor. * API mal diseñadas pueden permitir el acceso no autorizado a datos o funcionalidades. * La aplicación podría no estar preparada para resistir un ataque de denegación de servicio. | * Realizar pruebas de seguridad periódicas (pentesting, análisis de vulnerabilidades). * Implementar buenas prácticas de cifrado y manejo de autenticación. |
| **Riesgos Técnicos** | * Fallas de rendimiento * Compatibilidad * Errores en la lógica de negocio * Dependencia de terceros * Actualizaciones problemáticas | * Respuesta lenta o mal funcionamiento bajo cargas altas. * Problemas al ejecutarse en diferentes sistemas operativos, navegadores o dispositivos. * Bugs que provocan cálculos incorrectos o fallos en procesos críticos. * Problemas con librerías, APIs o servicios externos. * Cambios en la aplicación que generan errores o afectan negativamente a usuarios. | * Hacer pruebas de carga, rendimiento y compatibilidad. * Utilizar control de versiones y sistemas CI/CD para un desarrollo más seguro. |
| **Riesgos Operativos** | * Tiempo de inactividad * Gestión inadecuada de datos * Falta de escalabilidad | * Fallas del servidor o problemas de mantenimiento que afectan la disponibilidad. * Pérdida, corrupción o fuga de datos debido a copias de seguridad deficientes o mal manejo. * La aplicación no puede manejar un crecimiento en la cantidad de usuarios o datos. | * Diseñar sistemas redundantes y establece políticas de backup. * Monitorear continuamente el rendimiento y la disponibilidad. |
| **Riesgos Legales** | * Violación de privacidad * Propiedad intelectual * Términos de uso ambiguos | * No cumplir con regulaciones como RGPD, u otras leyes locales. * Uso indebido de contenido o código de terceros. * Problemas con las condiciones de uso o políticas de privacidad de la aplicación. | * Consultar a un experto legal para revisar términos, condiciones y regulaciones. * Asegurarse de tener permisos para usar contenido o bibliotecas externas. |
| **Riesgos de Negocio** | * Experiencia de usuario deficiente * Competencia * Mal manejo del feedback | * Diseño poco intuitivo que aleje a los usuarios. * Otra aplicación más eficiente o económica podría dominar el mercado. * Ignorar comentarios de los usuarios puede dañar la reputación de la aplicación. | * Realizar pruebas de usabilidad y escucha el feedback de los usuarios. * Analiza regularmente el mercado y la competencia. |
| **Riesgos Naturales Comunes** | * Terremotos * Huracanes o tormentas severas * Calor extremo * Nevadas o hielo * Inundaciones | * Daño a los servidores físicos en centros de datos o pérdida de conectividad si las infraestructuras de red se ven afectadas * Cortes de energía prolongados que pueden apagar servidores, daños físicos a instalaciones * Fallos en sistemas de enfriamiento de centros de datos, lo que puede llevar al sobrecalentamiento de los servidores * Interrupción en la logística y el mantenimiento de las infraestructuras críticas * Centros de datos afectados por el agua y Pérdida de hardware crítico y sistemas de almacenamiento | * Asegurarse de que los servidores estén ubicados en zonas de bajo riesgo natural, considera utilizar múltiples centros de datos geográficamente distribuidos * Implementar un sistema de copias de seguridad en diferentes ubicaciones, Usa servidores en la nube con soporte multi-región (ej. AWS, Azure, Google Cloud) * Realizar simulacros regulares para preparar al equipo frente a emergencias * Trabajar con proveedores que tengan infraestructuras resistentes, como generadores de respaldo, sistemas de enfriamiento redundantes y protección contra inundaciones |